Maryland Endpoint Protection Policy

Last Update: 01/31/2017

Contents

1.0 Purpose

Endpoint security management is an approach to network security that requires, and ensures, **endpoint devices** comply with specific criteria before being granted access to the network. Endpoint protection is an important aspect of maintaining the confidentiality, integrity, and availability of information. The increasing ease and prevalence of a mobile-enabled workforce makes it more important than ever to protect endpoint devices and the security posture of IT systems.

The Maryland Department of Information Technology (DoIT) will utilize baseline controls and standards established by NIST SP 800-53R4 and guidance provided by SP 800-128 to direct this policy.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013) Section 6.7: System and Information Integrity and 7.0 Access Control Requirements. This policy also supersedes any related policy regarding endpoint protection declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all endpoints devices (such as servers, workstations and mobile devices) utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. DoIT will be responsible for establishing endpoint protection and capabilities in accordance with the requirements in this policy, and for providing those capabilities to the Enterprise managed endpoints.

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

This policy describes an overall strategy to implement endpoint security within the Maryland Department of Information Technology infrastructure and executive agencies. Maryland DoIT, as well as agencies managing their own endpoints outside of the DoIT Enterprise, shall implement endpoint security by observing the requirements outlined in the sections below.

4.1 General Requirements

#	Name	Requirement
A	Endpoint Security	Protect and secure endpoint devices.

#	Name	Requirement
B	Process	Establish processes and rulesets for the configuration of endpoint devices.
C	Automated Endpoint Protection	Implement an automated endpoint security mechanism to support the protection and detection of endpoint devices, where possible.

4.2 Access Control

Access controls must be implemented at the software level (OS and API) as well as the device level (physical) to ensure endpoint protection. Agencies must establish access control in accordance with the requirements described below.

#	Name	Requirement
A	Least Privilege	Access should be limited to only those authorized users necessary to accomplish the assigned tasks in accordance with organization missions and business functions.
B	Privilege Levels	Establish non-privileged and privileged levels of users.
C	Privileged Access	Prevent non-privileged users from executing privileged functions, including disabling, circumventing, or altering implemented security safeguards and countermeasures.
D	Purge and Wipe Capabilities	Employ a ruleset that wipes information from select endpoint devices after an established number of consecutive, unsuccessful device log-in attempts.
E	Device-based Encryption	Employ full device or container encryption to protect the confidentiality and integrity of information on an endpoint device, where possible.

4.3 Audit and Accountability

Audit and logging must be implemented at the software level and device level to ensure endpoint protection. Audits must be conducted and logs maintained in accordance with the requirements described below.

#	Name	Requirement
A	Session Audit	Provides authorized users the capability to select a user session to capture or record.
B	System Start-up Audit	Provides capability to initiate session-audits at system start-up.
C	Capture and Log Content	Provides capability for authorized users to capture or record and log a user session content.

4.4 Endpoint Security Capabilities

Endpoint protection software should be configured to allow and perform the requirements outlined in the table below.

#	Name	Requirement
A	Prevent Program Execution	Prevent program execution in accordance with established blacklists and whitelists regarding software program usage and restrictions.
B	Unauthorized Programs (Blacklisting)	Identify software programs not authorized to execute on the endpoint devices.
C	Authorized Programs (Whitelisting)	Identify software programs authorized to execute on the endpoint devices. ▪ Where possible, a deny-all, permit by exception ruleset should be implemented on endpoint devices storing confidential information
D	Periodic Review of Rulesets	Review and update the list of authorized and unauthorized software programs at least annually.
E	Automated Unauthorized Component Detection	An automated mechanism detects the presence of unauthorized hardware, software, and firmware components on, or attempting to gain access to, an endpoint device and takes the following actions: ▪ Disables network access by such components ▪ Isolates the components ▪ Notifies DoIT SOC Staff or agency equivalent
F	Unauthorized Installation Alerts	An automated Endpoint Protection system alerts when the unauthorized installation of software is detected.
G	Privileged Status Permission Rights	Prohibit user installation of software without explicit privileged status.
H	Data Loss Prevention	Prevent unauthorized exfiltration of information across managed interfaces.
I	Host Intrusion Prevention System (HIPS) Capability	Implement host-based protection, such as up-to-date anti-malware, exploitation prevention, and host-based firewalls on information system components. Where possible, information system components include, but are not limited to: ▪ Workstations ▪ Servers ▪ Mobile devices ▪ Network devices
J	Antivirus	Implement software that will prevent, detect and remediate malware infections on individual computing devices and IT systems, and ensure definitions are up to date and downloaded from a vendor source.
K	Web-browsing Protection	Provide web-browsing protection, such as script, ad, and website blocking while browsing the Internet.
L	Aggregation of Notifications	Where possible, aggregate security notifications and alerts into a central analysis tool (e.g., **Security Information and Event Management (SIEM)**.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Other related policies include:

- Asset Management Policy
- Configuration Management Policy
- Mobile Device Policy

7.0 Definitions

Term	Definition
Endpoint Devices (endpoint)	Defined as a computer hardware device on a network such as, but not limited to: workstations (desktop computers, laptops, and thin clients), servers, smartphones, tablets, printers or other specialized hardware such Point of Sales (POS) terminals.
Endpoint Security	Approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources.
Security Information and Event Management (SIEM)	Application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing endpoint protection for Enterprise on-boarded agencies. DoIT will manage endpoint security according to established requirements authorized in the DoIT Cybersecurity Program Policy and described in this policy's section 4.0. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies. Any agencies under the policy authority of DoIT with requirements that deviate from the DoIT Cybersecurity Program policies are required to submit a Policy Exemption Form to DoIT for consideration and potential approval.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority,

may extend a non-compliant agency's window of resolution or authorize DoIT to shutdown external and internal network connectivity until such time the agency becomes compliant.

Any attempt by personnel to circumvent or otherwise bypass this endpoint protection policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written notice, suspension, termination, or possibly criminal and/or civil penalties.